国際標準化活動を振り返って

Journal of the Tokyo University of Marine Science and Technology, Vol. 10, pp. 3-5, 2014

［随想］

国際標準化活動を振り返って

（株）日本環境認証機構　新規事業推進部　佐藤　吉信

Looking Back on the International Activity for Standardization

Yoshinobu SATO

プロローグ

今年、2013 年は、日本列島周囲の海水温が通常より高温となったという。これが起因しているのであろうか、夏季を中心に各地で記録的な集中豪雨が各地で発生し、水害などの被害を多発させた。しかし、東京及び関東地区周辺では、むしろ夏場は少雨であり、首都圏貯水ダム渇水が心配された。8 月下旬に、渇水を心配している者にとっては慈雨ではあったが、筆者の住居周辺は激しい雷雨に襲われた。

その直後と推測されるが、住居で使用している三台のパソコンのうちの一台がインターネットに接続不可能となった。再設定などを繰り返し、懸命に通信の復帰を試みるのであるが、どうしても正常状態に回復できない。遂に、三台のパソコンと外部ネットワーク経路間を制御するルーターの電源を引き抜き、再投入したところ、イナターネットへの接続が自動的に復帰した。

電子機器、とりわけコンピュータが関連する電子機器は年々その機能を驚くべき速度で向上させている。これにともない、電子回路はその微細化を高め、組み込みソフトはより複雑化している。雷等による電磁ノイズの影響とこれに対応するソフトウェアとの関係により、通信障害が起きても不思議ではない。たまたま、障害が起きたものは A 社の OS（Operating System）を用いた製品であり、障害が起きなかったものは I 社の OS を用いた製品である。同一の OS を用いていたならば、全てのパソコンのネットワークへの接続が同時に不能となった可能性があり、不便な思いをしたことであろう。

さて、筆者は 1992 年 4 月に東京商船大学交通電子制御工学講座に赴任して以来、学部では制御機器工学、プラント管理、信頼性工学、情報管理システム等の科目、大学院では機能安全工学、リスク管理工学等の科目を担当し、大変勉強させていただいた。赴任と同時に、横浜国立大学大学院の科目であるリスク分析論の非常勤講師も務めることとなった。1993 年の新学期が始まったころ、リスク分析論の講義を行うため国大の廊下を歩いていたところ、S 教授（現名誉教授）とお会いした。国際標準化の作業としてシステム安全関連の規格開発の作業の必要性ができたので協力してくれないかという趣旨の話をされた。

そのころ、筆者はすでに IEC（国際電気標準会議）ディペンダビリティ（信頼性）に関する技術委員会（IEC TC56）のエキスパートであったので、国際標準化の作業がどのようなものなのかはある程度理解していた。システム安全は、二つ以上の要素の相互干渉により安全性が損なわれる場合に、それらの要素間の関係を調べ、リスクを評価し、また安全のための方策を見出す専門分野である。大学へ赴任する前は、産業安全研究所において産業災害の原因調査、システム安全などの課題を 18 年にわたり手掛け、とりわけ「人間―ロボット系の安全性評価」という題名で学位を取得したこともあり、システム安全には非常に心惹かれるものがあったのである。

早速、国内対策委員会が（社）電気計測器工業会に設置され、S 教授が国内対策委員会主査、筆者が幹事という役柄で日本としての対応が始まった。問題のシステム安全関連の規格は、IEC 61508「電気・電子・プログラマブル電子安全関連系の機能安全」（翻訳名）という題名であることがわかった。これは IEC TC65 SC A に設置された作業部会が担当して 1990 年頃から開発を開始したものである。IEC TC65 は計測と制御に関する国際標準化を行う技術委員会で、SC A はシステムの観点から計測と制御の課題を扱う技術部会である。

20 世紀後半にコンピュータが実用化された。当初コンピュータ技術は、生産、プロセスの制御など安全には直接関わらない分野で用いられていた。しかし、20 世紀終盤には、例えば、高品質の製品を生産するために、プラントの生産プロセスの温度や圧力がプログラマブル電子機器により自動制御されるようになった。ところが、プログラマブル電子機器が温度や圧力の制御に失敗するとしばしば暴走反応による火災・爆発事故に至ることから、当該機器は温度や圧力の制御により事故を防ぐ安全機能をも遂行しているとみなされることになる。当時、安全確保の観点から、このようなプログラマブル電子機器

をどのように設計、開発、製造そして使用すべきかのガイドラインがどの国、いかなる団体にも存在していなかった。そこで、英国、ドイツ、米国を中心として IEC 61508 規格の開発が着手されたのである。

S 教授とともに、初めて IEC 61508 規格開発会議に出向いたのは翌年の 6 月であったであろう。英国のリバプール近郊のブートルに位置する HSE（健康安全庁）の会議室が会場であった。リバプールのホテルに宿泊して、電車で HSE に通った。この規格開発の主査 R. Bell は、現役の HSE の電子安全部門の責任者でもあった。夕刻の 10 時半になっても外は明るく、Bell の自宅に招待されたりもした。当時は、北アイルランド紛争が完全には終結しておらず、HSE の建屋のセキュリティは非常に厳しいものがあった。建物に入る際のチェック、廊下から部屋に入る際、部屋から廊下に出る際、廊下から洗面室に入る際、洗面室から廊下に出る際にはすべて暗証番号によりドアーの開閉が規制されていた。（後日談である。HSE はその後 10 年あまり経過した後、建屋を新築した。日本の有名な K 建設が設計施工したことが記されていた。地震がない国柄からか、柱がマッチ棒のように細く、内部は商店街のアーケードのようで、だれもがどこでも自由に出入りできる開放的なデザインになった。）最初のころの会議の思い出は、以上のようなもののみであり、議論した内容はほとんど覚えていない。

以降、規格開発会議が年に 2 ～ 3 回程度ドイツ、フランス、オランダ、英国、米国、ノルウェー、イタリア、日本などに会場を移して開催された。規格開発会議にはエキスパートと呼ばれる各国代表者が出席して討議する。エキスパートは、少ない国で 1 ～ 2 名、多い国で 5 ～ 6 名である。エキスパートの得意分野は、ハードウェア、ソフトウェア、システム、プロセスマネジメント、リスクアセスメントなどに分かれる。会議の 2 ～ 3 日程度は、ソフトウェアとハードウェア / システムとに分かれて問題点について議論し、最後の日に全体会議で整合及び統合をはかることになる。当初は電子メールが普及し始めた段階であり、会議では OHP 及び紙媒体が使用されていた。やがて、パソコンによる映写のスタイルに移行した。

エキスパートの出身母体は、行政 / 研究所 / 第三者機関などから若干名、英国の BP 社、ドイツの BASF 社 / バイエルン社、フランスのトタール社、米国のシェル社 / ディポン社などのプロセス産業界から半数、その他安全計装システムのメーカー技術者から構成され、大学からは筆者らのみが参加に与った。紆余曲折して、2000 年には IEC 61508 第一版を出版し、2010 年には改正第 2 版を発行することができた。筆者は、1993 年から規格開発に参加したことになるが、規格原案の全体像をある程度把握、理解するまでに 2 ～ 3 年が必要であった。

上述したように、錚々たるメンバーが討議しながら規格を開発していくのであるが、かれらの実務面での知識と経験の豊富さには驚嘆すべきものがあった。筆者は、産業安全研究所での産業災害の原因調査業務等で我が国の産業界の安全技術又は安全文化のレベルについてはかなり把握していた。日本が先進国の一級の安全レベルに到達するにはおそらく 30 年は必要であろうし、その間に先進国の安全技術 / 文化が進捗していれば、永久に追い越すことはできないのではないかと思えた。産業革命において、日本は欧米よりも 1 世紀出遅れたことになる。技術面のみであれば、追いつき又は追い越した分野があるかもしれない。しかし、安全文化など根底となる意識面の変革は困難であり、長い時間が必要であるように感じられた。

毎回、会議に挑戦的な精神で参加した。すると参加するたびに様々な問題、特にリスクアセスメントに関する課題を自ずから頂戴することができた。機能安全規格の方法論そのものが斬新であり、未踏の分野でもあった。課題を忘れないように記録して、大学に戻った。そして、それらの課題を早速、卒論、修論、博士論文の研究テーマとすることができた。こうして、1998 年前後から 2010 年頃の間に機能安全の分野で 10 編程度の博士学位論文の作成指導を行うことができた。これは大変に幸運なことであったと思っている。

現在、IEC 61508 は、基本安全規格として、各種の分野あるいは製品の機能安全規格の開発及び発行を促している。それらは、IEC 61511（プロセス産業分野）、IEC 62061（産業機械類）、IEC 61513（原子力分野）、IEC 62279（鉄道分野）、ISO 26262（自動車電子制御）、ISO 13482（パーソナルケアロボット）、IEC 60601（医療機器の機能安全）などを含む。特に、今後 10 年程度以内に完全自動走行の自動車が ISO 26262 等の機能安全の枠組みによって実用化されるであろうことが想定されている。

エピローグ

膨大な知識・情報が刻々と新たに生産されているものの、個人的レベルでも社会集団的レベルにおいても、その時点における知識には限界が存在する。これが想定外の故障 / 失敗が存在する所以である。すなわち、我々は既知なる (Known) 分野と未知なる (Unknown) の分野とに同時に生存している。安心 (Psychological Security) は既知の領域にあり、自己が生命、知識、財産などを所有している、すなわち自己が関係していると考えているもの、それらは社会、自然界、家族など多岐にわたるが、それらが持続・存続することの確かさとも定義できる。仮に、所有関係が存続できない、あるいは部分的にも関係が毀損される可能性があると感じれば不安 (Anxiety) に、さらにその可能性を確信すれば恐れ (Fear) につながるかもしれない。しかし、未知の領域では、漠然とした不安 (Unanchored) が存在するのみである。例えば、我々は「死」を恐れるというかもしれないが、死が未知の領域にあるとすれば、実際は死そのものを恐れることはできない。死を恐れるのではなく自己が既知の関係を喪失することを恐れているとも解釈できる。

我国においても、高度成長期以前においては、安心という言葉は一部の宗教的な活動では使用されていたものの、学術団体等において使用されたことは皆無であったであろう。宗教的な色彩をもつ安心という言葉が学術団体においても多用されるようになったのは、我国が世界第二位の経済大国になって後のことである。

「安全・安心」と一区切りの単語として用いる場合の安心は、持続・継続性あるいは社会的秩序性を意味しており、何らかの宗教的な意味をもつものではないことは明らかである。例えば、宗教的に「安心立命に至る」などといった場合の安心は、社会的秩序性としての持続・継続性とは異なり、逆に自己の持続・継続性からの解放という意味になる。

現在、安全・安心あるいは「安心・安全」という標語が政治的，社会的あるいは学術的に広く用いられている。研究計画書に安心という文言が入らないと、安全関連研究の研究費の確保もままならない時代である。この経緯は次のようにも解釈できる。すなわち、安全性の達成には努力、コスト、その他諸々の面倒なことが付随するので、単に「安全にすべきである」あるいは「安全性を達成すべきである」といっても実行上の効果が乏しいことは明らかである。反面、「安全・安心」といえば、安全でない場合の不安・恐れがすぐさま想像でき、安全であることによる不安や恐れからの解放すなわち安心という報酬のイメージが我々を虜にし、強力に安全性達成上の心理的な動機につながる。これが「安全・安心」の安全確保上の大きな肯定的側面である。

安心・安全は既知の領域に存在し、この領域に自己満足して安住することで、ある種の心地よさを得られるかもしれない。しかし、安心・安全に安住していると、未知の領域からの挑戦に対する油断という落とし穴にはまる負の側面があるので注意を要する。我々は、既知と未知との世界に併存しており、世界は常に変化し、想定外という形式で我々に挑戦状を投げかけてくる。これに即座に対応できなければ安全は確保できない。これには、研ぎすまされた神経により前兆を感じとる感覚の信頼性、知識の信頼性、実行力の信頼性、マネジメントの信頼性など多様な信頼性の確保が必須となる。このような多様な信頼性の確保による安全が機能安全である。